Finite Fields and Their Applications 15 (2009) 615–632

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

When does $G(x) + \gamma\, Tr(H(x))$ permute $\mathbb{F}_{p^n}$?

Pascale Charpin [a], Gohar Kyureghyan [b,*]

[a] *INRIA, SECRET Research Team, B.P. 105, 78153 Le Chesnay Cedex, France*
[b] *Otto-von-Guericke University Magdeburg, Department of Mathematics, Universitatplatz 2, Magdeburg, Germany*

ARTICLE INFO

Article history:
Received 7 November 2008
Revised 8 June 2009
Available online 4 August 2009
Communicated by Gary L. Mullen

Keywords:
Permutation polynomial
Linear permutation
p-to-1 mapping
Linear structure
Linear space
Boolean function

ABSTRACT

We study permutation polynomials of the shape $G(X)+\gamma\, Tr(H(X))$ in $\mathbb{F}_{p^n}[X]$. Using a link with functions having a linear structure, we introduce an effective method to construct many such permutations, as well as p-to-1 mappings.

1. Introduction

Let p be a prime number and $\mathbb{F}_{p^n}$ be the finite field of order p^n. Any polynomial $F(X) \in \mathbb{F}_{p^n}[X]$ defines a mapping

$$F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$$
$$x \mapsto F(x),$$

which is called the associated mapping of $F(X)$. Recall that any mapping of a finite field into itself is given by a polynomial. In this paper we write F or $F(x)$ to denote a mapping, while $F(X)$ is reserved for a polynomial. Also, we generally use the term "mapping" to refer $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, while we use "function" for $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$.

A polynomial $F(X)$ is called a *permutation polynomial* of $\mathbb{F}_{p^n}$ if the mapping F is a permutation of $\mathbb{F}_{p^n}$. The construction of infinite classes of permutation polynomials over finite fields is an interest-

* Corresponding author.
E-mail addresses: pascale.charpin@inria.fr (P. Charpin), gohar.kyureghyan@mathematik.uni-magdeburg.de (G. Kyureghyan).

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2009.07.001

ing and widely open problem, which is of great importance for a variety of theoretical and practical applications.

This paper is motivated by the question: What happens when a permutation is *slightly* modified? The "slight modification" considered here is the addition of a *simple* mapping to a given permutation. In some sense our approach is related to the concept of complete mapping polynomials, where new permutations are obtained by adding the identity mapping. More precisely, a polynomial $F(X)$ is called a *complete mapping polynomial* if both $F(X)$ and $F(X)+X$ are permutation polynomials of $\mathbb{F}_{p^n}$. These polynomials were introduced by Niederreiter and Robinson in [20]. The study of general properties of the complete mapping polynomials seems to be very difficult (for recent results see [16]).

In this paper we consider polynomials of the shape

$$F(X) = G(X) + \gamma\, Tr\big(H(X)\big), \tag{1}$$

where $Tr(X)$ is the polynomial defining the absolute trace function of $\mathbb{F}_{p^n}$, $\gamma \in \mathbb{F}_{p^n}$ and $G(X)$, $H(X)$ are arbitrary polynomials in $\mathbb{F}_{p^n}[X]$. Examples of such permutation polynomials over $\mathbb{F}_{2^n}$ are obtained in [10,23] and [4].

A mapping $F:\mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is called *perfect nonlinear or planar* if for every nonzero $\alpha \in \mathbb{F}_{p^n}$ the difference mapping $x \mapsto F(x+\alpha) - F(x)$ is a permutation of $\mathbb{F}_{p^n}$. Perfect nonlinear mappings exist if and only if p is odd. If $p=2$, a mapping $F:\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called *almost perfect nonlinear* (*APN*) if all its difference mappings are 2-to-1. In [2,8,14] (almost) perfect nonlinear mappings of shape (1) are constructed. In [8] the construction of F from G is called the *switching construction*.

In this paper we point out a link between the concept of a *linear structure* and permutation polynomials of the form (1), which yields large classes of such permutation polynomials. The concept of a linear structure was introduced in cryptography, mainly for Boolean functions. A nonzero $a \in \mathbb{F}_{p^n}$ is called a linear structure of a Boolean function f if the derivative of f at the point a is constant. Such a property is considered as a weakness in some cryptographic applications ever since the cryptanalysis suggested by Evertse in [9], which exploits the existence of linear structures. Later in [19] the notion of the *nonlinearity of f with respect to a linear structure* was introduced to quantify the distance of f to any linear structure (see also [5]). This nonlinearity is invariant under the general affine group, and therefore seems to be a *useful cryptographic criterion*. Linear structures were extensively studied in [7] and [15]. A partial classification of the monomial and binomial functions with linear structures is given in [12,1].

This paper is organized as follows. In Section 2 background and preliminary results on functions with linear structures are given. Section 3 starts with a general study on permutation polynomials of shape (1). Propositions 3 and 4 give necessary conditions on $\gamma \in \mathbb{F}_{p^n}$, $G(X)$ and $H(X)$ for which $G(X) + \gamma\, Tr(H(X))$ is a permutation polynomial. These conditions appear to be very effective in proving that a certain polynomial of shape (1) is not a permutation polynomial, as demonstrated in Examples 1, 2. Section 3.1 is devoted to the permutations of form (1), where G is itself a permutation. Theorem 3 gives a sufficient condition on γ and $H(X)$ ensuring that F is either a permutation or a p-to-1 mapping. Using this theorem and results from Section 2, Corollary 1 describes two large classes of permutation polynomials of $\mathbb{F}_{p^n}$.

In Section 3.2 it is assumed that $G(X)$ is a linearized polynomial inducing a p-to-1 mapping. The notation $L(X)$ is used for such a $G(X)$ for clarity. Theorem 4 characterizes the permutation polynomials of shape (1) obtained with such an $L(X)$. Theorem 5 gives a sufficient condition on $\gamma \in \mathbb{F}_{p^n}$, $L(X)$ and $H(X)$ to induce a permutation polynomial $L(X) + \gamma\, Tr(F(X))$. This theorem and results from Section 2 are applied to describe two large classes of permutation polynomials of $\mathbb{F}_{p^n}$ in Corollary 2. Finally, Theorem 6 allows to obtain the dimension of the kernel of a linear mapping $L(x) = L_1(x) + \gamma\, Tr(\beta x)$ from the one of $L_1(x)$. An application of Theorem 6 is demonstrated in Example 4 to construct explicitly linearized polynomials inducing p-to-1 mappings. In Section 4 the results of the previous sections are applied to characterize the linearized permutation polynomials of shape (1). Moreover, a large family of linearized permutation polynomials over binary finite fields is obtained via semi-bent Boolean functions.

Notation: We denote by $|E|$ the cardinality of a set E. The trace function from $\mathbb{F}_{p^n}$ onto any subfield $\mathbb{F}_{p^k}$ of $\mathbb{F}_{p^n}$ will be denoted as follows:

$$Tr_{n/k}(y) = y + y^{p^k} + \cdots + y^{p^{k(n/k-1)}}.$$

The absolute trace function (*i.e.*, $k = 1$) is simply denoted by Tr.

2. A linear structure

In this section we consider functions from a finite field $\mathbb{F}_{p^n}$ into its prime subfield $\mathbb{F}_p$. Every function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ can be represented by $Tr(R(x))$ for some (not unique) mapping $R : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$.

Definition 1. Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ and $c \in \mathbb{F}_p$. We say that $\alpha \in \mathbb{F}_{p^n}^*$ is a c-linear structure of the function f if

$$f(x+\alpha) - f(x) = c \quad \text{for all } x \in \mathbb{F}_{p^n}. \tag{2}$$

Note that if α is a c-linear structure of f, then necessarily $c = f(\alpha) - f(0)$. The next proposition is proved in [15]; we included its proof for clarity.

Proposition 1. *Let $\alpha, \beta \in \mathbb{F}_{p^n}^*$, $\alpha + \beta \neq 0$ and $a, b \in \mathbb{F}_p$. If α is an a-linear structure and β is a b-linear structure of a function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$, then*

$$\alpha + \beta \text{ is an } (a+b)\text{-linear structure of } f$$

and for any $c \in \mathbb{F}_p^*$

$$c \cdot \alpha \text{ is a } (c \cdot a)\text{-linear structure of } f.$$

In particular, if Λ^* is the set of linear structures of f, then $\Lambda = \Lambda^* \cup \{0\}$ is an $\mathbb{F}_p$-linear subspace, which we call the linear space *of f.*

Proof. Let $\alpha, \beta \in \Lambda^*$, where α is an a-linear structure and β a b-linear structure. Then for any $x \in \mathbb{F}_{p^n}$ it holds

$$\begin{aligned} f\big(x + (\alpha+\beta)\big) - f(x) &= f\big((x+\alpha)+\beta\big) - f(x+\alpha) + f(x+\alpha) - f(x) \\ &= a + b. \end{aligned}$$

Thus $\alpha + \beta \in \Lambda$ and a nonzero $\alpha + \beta$ is an $(a+b)$-linear structure of f. Further, taking $\beta = \alpha$ we get that 2α belongs to Λ and 2α is a $2a$-linear structure. Similarly, $c\alpha$ is a ca-linear structure for any $c \in \mathbb{F}_p^*$, completing the proof. □

Given $\gamma \in \mathbb{F}_{p^n}^*$ and $c \in \mathbb{F}_p$, let $\mathcal{H}_\gamma(c)$ denote the affine hyperplane defined by the equation $Tr(\gamma x) = c$, *i.e.*,

$$\mathcal{H}_\gamma(c) = \big\{x \in \mathbb{F}_{p^n} \;\big|\; Tr(\gamma x) = c\big\}. \tag{3}$$

Then $\alpha \in \mathbb{F}_{p^n}^*$ is a c-linear structure of $Tr(R(x))$ if and only if the image set of the mapping $R(x+\alpha) - R(x)$ is contained in the affine hyperplane $\mathcal{H}_1(c)$.

Let $\xi \in \mathbb{C}$ be a p-th root of unity. For a given $R : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, let $\mathcal{F}_R : \mathbb{F}_{p^n} \to \mathbb{C}$ be defined by

$$\mathcal{F}_R(\lambda) = \sum_{x \in \mathbb{F}_{p^n}} \xi^{Tr(R(x)-\lambda x)}. \tag{4}$$

The mapping $\mathcal{F}_R$ is the *discrete Fourier transform* of the mapping

$$x \in \mathbb{F}_{p^n} \mapsto \xi^{Tr(R(x))} \in \mathbb{C}.$$

In particular, $\mathcal{F}_R = \mathcal{F}_{R'}$ if and only if the functions $Tr \circ R$ and $Tr \circ R'$ are equal. Set $f = Tr \circ R$. We say that $\mathcal{F}_R$ is the *Fourier transform* of f. And we call the multiset

$$S(f) = \left\{ \mathcal{F}_R(\lambda) \;\middle|\; \lambda \in \mathbb{F}_{p^n} \right\}$$

the *Fourier spectrum* of f. Whether f has a linear structure can be recognized from a property of $S(f)$. The following proposition is known for $p = 2$ (see [22] and [7]). Here we extend it for an arbitrary prime p.

Proposition 2. *Let $c \in \mathbb{F}_p$, $R : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and $f(x) = Tr(R(x))$. An element $\alpha \in \mathbb{F}_{p^n}^*$ is a c-linear structure for f if and only if*

$$\mathcal{F}_R(\lambda) = 0 \quad \text{for all } \lambda \notin \mathcal{H}_\alpha(c). \tag{5}$$

Proof. Recall that $\alpha \in \mathbb{F}_{p^n}^*$ is a c-linear structure for f if and only if

$$Tr\big(R(x+\alpha)\big) - Tr\big(R(x)\big) = c \quad \text{for all } x \in \mathbb{F}_{p^n}.$$

This holds if and only if, for some $\beta \in \mathbb{F}_{p^n}$ such that $Tr(\beta) = c$,

$$\mathcal{F}_R = \mathcal{F}_{R'} \quad \text{with } R'(x) = R(x+\alpha) - \beta.$$

Further, observe that

$$\begin{aligned} \mathcal{F}_{R'}(\lambda) &= \sum_{x \in \mathbb{F}_{p^n}} \xi^{Tr(R(x+\alpha)-\beta-\lambda x)} \\ &= \xi^{Tr(\alpha\lambda)-c} \sum_{x \in \mathbb{F}_{p^n}} \xi^{Tr(R(x+\alpha)-\lambda(x+\alpha))} \\ &= \xi^{Tr(\alpha\lambda)-c} \mathcal{F}_R(\lambda). \end{aligned}$$

Thus $\mathcal{F}_R = \mathcal{F}_{R'}$ if and only if $\mathcal{F}_R(\lambda) = 0$ for all $\lambda \in \mathbb{F}_{p^n}$ such that $Tr(\alpha\lambda) - c \neq 0$, *i.e.*, for all λ which are not in the affine hyperplane $\mathcal{H}_\alpha(c)$. □

In [15], Lai uses the multivariable representation to characterize the functions assuming a linear structure. Here we state this result for the univariable representation.

Theorem 1. *Let $R : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and $f = Tr \circ R$. Then f has a linear structure if and only if there is a nonbijective linear mapping $L : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ such that*

$$f(x) = Tr\big(R(x)\big) = Tr\big(H \circ L(x) + \beta x\big) \tag{6}$$

for some $H : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and $\beta \in \mathbb{F}_{p^n}$. In this case, the linear space of f contains the kernel of L.

Proof. The statement is obviously true if f is affine; we may take L to be the zero mapping for such an f. For the rest of the proof we assume that f is nonaffine. Suppose that (6) holds and α is an arbitrary element from the kernel of L. Then α is a linear structure of f. Indeed,

$$\begin{aligned} f(x+\alpha) - f(x) &= Tr\big(H\big(L(x)+L(\alpha)\big)\big) - Tr\big(H\big(L(x)\big)\big) + Tr(\beta\alpha) \\ &= Tr(\beta\alpha), \end{aligned}$$

since $L(\alpha) = 0$.

Conversely, suppose that there exist $\alpha \in \mathbb{F}_{p^n}^*$ and $c \in \mathbb{F}_p$ such that $f(x+\alpha) - f(x)$ is constantly equal to c. This means that the linear space Λ of f has dimension $k \geqslant 1$ (see Proposition 1). Moreover, $k \leqslant n-1$ because of the assumption that f is nonaffine. Let $\{\alpha_1, \ldots, \alpha_k\}$ be a basis of Λ and α_i be a c_i-linear structure of f. Then choose $\beta \in \mathbb{F}_{p^n}$ such that

$$Tr(\beta\alpha_i) = c_i, \quad 1 \leqslant i \leqslant k, \tag{7}$$

which exists always. Indeed, such a β belongs to the intersection of the affine hyperplanes $\mathcal{H}_{\alpha_i}(c_i)$, which is not trivial, because $1 \leqslant k \leqslant n-1$ and the choice of α_i. Further choose a linear mapping L with the kernel Λ. Note that L is not bijective since $k \geqslant 1$. Finally, define a function $H : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ as follows:

(a) For any $y \in \mathbb{F}_{p^n}$, such that $y = L(x)$ for some $x \in \mathbb{F}_{p^n}$, the value $H(y)$ satisfies $Tr(H(y)) = f(x) - Tr(\beta x)$.
(b) For $y \in \mathbb{F}_{p^n}$ which is not in the image set of L the value $H(y)$ is arbitrary.

It remains to show that such an H is well defined, that is for any $x \in \mathbb{F}_{p^n}$ and $x' \in \mathbb{F}_{p^n}$ it holds

$$L(x) = L(x') \quad \Rightarrow \quad Tr\big(H\big(L(x)\big)\big) = Tr\big(H\big(L(x')\big)\big).$$

So we must prove that if $L(x-x') = 0$ then $Tr(\beta x') - Tr(\beta x) = f(x') - f(x)$. Note that $L(x-x') = 0$ implies that $x' = x + \alpha$ with $\alpha \in \Lambda$. Let $\alpha = \sum_{i=1}^{k} a_i\alpha_i$, $a_i \in \mathbb{F}_p$. Then Proposition 1 yields that α is a c-linear structure of f with $c = \sum_{i=1}^{k} a_i c_i$. Thus

$$f(x') - f(x) = f(x+\alpha) - f(x) = c.$$

To complete the proof note that from (7) it follows

$$Tr\big(\beta(x'-x)\big) = Tr(\beta\alpha) = \sum_{i=1}^{k} a_i\, Tr(\beta\alpha_i) = c. \qquad \square$$

Theorem 1 shows that any linear mapping with a known kernel allows to construct a function with (at least partly) known linear space. The following result is an example of this.

Lemma 1. *Let $H : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be an arbitrary mapping, $\gamma, \beta \in \mathbb{F}_{p^n}$, $\gamma \neq 0$ and $c = Tr(\beta\gamma)$. Then γ is a c-linear structure of $f(x) = Tr(R(x))$ where*

$$R(x) = H\big(x^p - \gamma^{p-1}x\big) + \beta x.$$

Proof. Since $R(x+\gamma) = H(x^p + \gamma^p - \gamma^{p-1}x - \gamma^p) + \beta x + \beta\gamma = R(x) + \beta\gamma$, we have

$$Tr\big(R(x+\gamma) - R(x)\big) = Tr(\beta\gamma) = c \quad \text{for all } x \in \mathbb{F}_{p^n}. \qquad \square$$

The next lemma describes another family of functions with a known linear structure.

Lemma 2. *Let $g:\mathbb{F}_{p^n}\to\mathbb{F}_p$ and $\alpha\in\mathbb{F}_{p^n}^*$. Then for any $c\in\mathbb{F}_p^*$ the element $c\alpha$ is a 0-linear structure of*

$$f(x)=\sum_{u\in\mathbb{F}_p} g(x+u\alpha).$$

Proof. Indeed, $f(x+c\alpha)=\sum_{u\in\mathbb{F}_p} g(x+\alpha(u+c))=f(x)$. □

3. Permutation polynomials

For the remainder of this paper, we consider the polynomials of the shape

$$F(X)=G(X)+\gamma\, Tr\big(H(X)\big), \tag{8}$$

where $G(X), H(X)\in\mathbb{F}_{p^n}[X]$, $\gamma\in\mathbb{F}_{p^n}$. Our main goal is to characterize and construct such permutation polynomials. Firstly, we give two simple necessary conditions on γ, G and H, for which the corresponding F is a permutation. These conditions appear to be very effective in proving that a certain polynomial of shape (8) is not a permutation polynomial. For instance, by Proposition 3 if $F(x)$ is a permutation then the image set of $G(x)$ must be of size at least p^{n-1}.

Proposition 3. *Let $F(X)\in\mathbb{F}_{p^n}[X]$ be a polynomial of type* (8)*. Assume that $F(x)$ is a permutation. Then for any $\beta\in\mathbb{F}_{p^n}$ there are at most p elements $x\in\mathbb{F}_{p^n}$ with $G(x)=\beta$.*

Proof. Suppose that $G(x_i)=\beta$ for $i=1,\dots,p+1$, where x_i are pairwise different. Then for these x_i we have:

$$F(x_i)=\beta+\gamma c \quad \text{with } c\in\mathbb{F}_p,$$

providing at most p different values. Thus $F(x)$ cannot be a permutation. □

Proposition 3 implies that if a k-to-1 mapping G yields a permutation of shape (8), then $k\leqslant p$. The following example is based on this observation.

Example 1. Let $3\leqslant s\leqslant p^n-2$ be such that $\gcd(s,p^n-1)=d$ and $d>p$. Then for any $\lambda,\gamma\in\mathbb{F}_{p^n}^*$ and for any $H:\mathbb{F}_{p^n}\to\mathbb{F}_{p^n}$ the mapping

$$F(x)=\lambda x^s+\gamma\ Tr\big(H(x)\big)$$

is not a permutation. Indeed, the mapping $x\mapsto x^s$ is d-to-1, and then Proposition 3 implies the result.

Note that d is odd, if $p=2$. Consequently, if the mapping F is a permutation then necessarily $d=1$, or equivalently, the mapping $x\to x^s$ is a permutation.

We extend the previous proposition as follows:

Proposition 4. *Let $F(X)$ be a permutation polynomial of type* (8) *and $F(0)=0$. Then for any nonzero $x\in\mathbb{F}_{p^n}$ satisfying $G(x)=\gamma c$ for some $c\in\mathbb{F}_p$ it must hold $Tr(H(x))\neq -c$.*

Proof. Since $F(0)=0$ and $F(x)$ is a permutation, $F(x)\neq 0$ for any nonzero x, or equivalently,

$$G(x)+\gamma u\neq 0 \quad \text{where } u=Tr\big(H(x)\big).$$

Thus if for some $x\neq 0$ it holds $G(x)=\gamma c$ with $c\in\mathbb{F}_p$, then $Tr(H(x))\neq -c$. □

Example 2. Let a mapping F of $\mathbb{F}_{p^n}$ be defined by

$$F(x) = G(x) + \gamma\, Tr\big(H(x)\big).$$

Moreover, let $F(0) = G(0) = 0$, $\gamma \in \mathbb{F}_p^*$ and

$$G(\mathbb{F}_p) = \mathbb{F}_p, \qquad H\big(\mathbb{F}_p^*\big) = \{\beta\} \quad \text{with } Tr(\beta) \neq 0.$$

Then for any $c \in \mathbb{F}_p^*$ we have $F(c) = G(c) + \gamma\, Tr(\beta)$. By the assumption that G is a permutation on $\mathbb{F}_p$, there is $c \in \mathbb{F}_p^*$ such that $G(c)$ equals $-\gamma\, Tr(\beta)$ implying $F(c) = 0$. Thus, such a mapping F is not a permutation.

Recall that any polynomial $F(X) \in \mathbb{F}_{p^n}[X]$ is a permutation polynomial if and only if its associated mapping satisfies

$$\mathcal{F}_{\lambda F}(0) = \sum_{x \in \mathbb{F}_{p^n}} \xi^{Tr(\lambda F(x))} = 0 \quad \text{for all } \lambda \in \mathbb{F}_{p^n}^*, \tag{9}$$

where $\xi \in \mathbb{C}$ is a p-th root of unity (see for instance [17, Theorem 7.7]). In the next proposition this property is specified for the polynomials considered here.

Proposition 5. *Let $F(X) \in \mathbb{F}_{p^n}[X]$ be a polynomial of type* (8)*. Then*

$$F(x) = G(x) + \gamma\, Tr\big(H(x)\big)$$

is a permutation if and only if for any $\lambda \in \mathbb{F}_{p^n}^*$ it holds

$$\sum_{x \in \mathbb{F}_{p^n}} \xi^{Tr(\lambda G(x) + cH(x))} = 0 \quad \textit{where } c = Tr(\gamma\lambda). \tag{10}$$

Proof. We simply apply the necessary and sufficient condition (9). Since

$$\begin{aligned} Tr\big(\lambda F(x)\big) &= Tr\big(\lambda G(x)\big) + Tr\big(H(x)\big)\, Tr(\gamma\lambda) \\ &= Tr\big(\lambda G(x) + H(x)\, Tr(\gamma\lambda)\big), \end{aligned}$$

condition (9) becomes

$$\sum_{x \in \mathbb{F}_{p^n}} \xi^{Tr(\lambda G(x) + cH(x))} = 0 \quad \text{where } c = Tr(\gamma\lambda). \qquad \square$$

Next we consider polynomials $F(X)$ of type (8) where $G(X)$ is a permutation or a linearized polynomial. In both cases, we will show that the existence of linear structures provides permutations under certain conditions.

Open Problem 1. Characterize a class of permutation polynomials of type (8), where $G(X)$ is neither a permutation nor linearized polynomial.

3.1. Permutations from permutations

Here we consider polynomials of shape (8) under additional assumption that $G(X)$ is a permutation polynomial. We establish a link between such permutation polynomials and the existence of a linear structure for certain functions. As a consequence, we construct large classes of permutation polynomials.

Theorem 2. *Let $\gamma \in \mathbb{F}_{p^n}$, $G(x)$ be a permutation on $\mathbb{F}_{p^n}$ and $H : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be an arbitrary mapping. Then the mapping*

$$F(x) = G(x) + \gamma\ Tr\big(H(x)\big)$$

is a permutation on $\mathbb{F}_{p^n}$ if and only if for any $\lambda \in \mathbb{F}_{p^n}$ with $Tr(\gamma\lambda) = c$, $c \in \mathbb{F}_p^*$, it holds

$$\mathcal{F}_{cR}(-\lambda) = \sum_{y \in \mathbb{F}_{p^n}} \xi^{Tr(cR(y)+\lambda y)} = 0, \tag{11}$$

where $R = H \circ G^{-1}$ and G^{-1} is the inverse mapping of G.

Proof. Since $G(x)$ is a permutation, (10) is satisfied for $c = 0$. Further we show that (10) is equivalent to (11) for $c \neq 0$. Firstly, note that

$$\sum_{x \in \mathbb{F}_{p^n}} \xi^{Tr(\lambda G(x)+cH(x))} = \sum_{y \in \mathbb{F}_{p^n}} \xi^{Tr(cH(G^{-1}(y))+\lambda y)} = \mathcal{F}_{cR}(-\lambda).$$

So (10) holds if and only if $\mathcal{F}_{cR}(-\lambda) = 0$ for any $c \neq 0$ and for any λ with $Tr(\lambda\gamma) = c$. □

Remark 1. When $p = 2$, the statement of Theorem 2 can be rewritten as follows: $F(x)$ is a permutation if and only if $\mathcal{F}_R(\lambda) = 0$ for any $\lambda \in \mathbb{F}_{2^n}$ with $Tr(\gamma\lambda) = 1$, or equivalently, if and only if γ is a 0-linear structure of $Tr(R(x))$ (see Proposition 2). More details on the binary case are given in [4].

Theorem 2 and Proposition 2 lead to a set of permutations obtained by means of functions having linear structures.

Theorem 3. *Let $G(x)$ be a permutation of $\mathbb{F}_{p^n}$. Let R be a mapping of $\mathbb{F}_{p^n}$ such that $\gamma \in \mathbb{F}_{p^n}$ is a b-linear structure of $Tr(R(x))$. Then we have*:

(**i**) *$F(x) = G(x) + \gamma\, Tr(R(G(x)))$ is a permutation of $\mathbb{F}_{p^n}$ if $b \neq -1$.*
(**ii**) *$F(x) = G(x) + \gamma\, Tr(R(G(x)))$ is a p-to-1 mapping of $\mathbb{F}_{p^n}$ if $b = -1$.*

Proof. Firstly note that γ is a cb-linear structure of $Tr(cR(x))$ for any $c \in \mathbb{F}_p^*$. Then by Proposition 2, we have

$$\mathcal{F}_{cR}(\lambda) = 0 \quad \text{for any } \lambda \notin \mathcal{H}_\gamma(cb),$$

or equivalently,

$$\mathcal{F}_{cR}(-\lambda) = 0 \quad \text{for any } \lambda \notin \mathcal{H}_\gamma(-cb)$$

(where $\mathcal{H}_\gamma$ is defined by (3)). Recall that λ is not in $\mathcal{H}_\gamma(-cb)$ if and only if $Tr(\gamma\lambda) \neq -bc$. In particular, it shows that in the case $b \neq -1$ it holds $\mathcal{F}_{cR}(-\lambda) = 0$ when $Tr(\gamma\lambda) = c$. Theorem 2 completes the proof of (**i**).

Our next goal is to prove (**ii**). Let y_0 be an arbitrary fixed element from the image of F, say $y_0 = F(x_0)$ for some x_0. Then

$$y_0 = G(x_0) + \gamma\, Tr\big(R\big(G(x_0)\big)\big) = G(x_0) + \gamma u_0,$$

where $u_0 = Tr(R(G(x_0))) \in \mathbb{F}_p$. Consequently, $x_0 = G^{-1}(y_0 - \gamma u_0)$ and we have

$$\big\{x \in \mathbb{F}_{p^n} \bigm| F(x) = y_0\big\} \subseteq \big\{G^{-1}(y_0 - \gamma u) \bigm| u \in \mathbb{F}_p\big\}.$$

In particular, there are at most p elements x such that $F(x) = y_0$. On the other side, for any $u \in \mathbb{F}_p$ it holds $F(G^{-1}(y_0 - \gamma u)) = y_0$. Indeed, γ is a (-1)-linear structure of $Tr(R(x))$, implying that γu is a $(-u)$-linear structure of $Tr(R(x))$ by Proposition 1. Thus for any $u \in \mathbb{F}_p$ it holds

$$Tr\big(R(x + \gamma u)\big) - Tr\big(R(x)\big) = -u \quad \text{for all } x \in \mathbb{F}_{p^n}. \tag{12}$$

Hence we have

$$\begin{aligned} F\big(G^{-1}(y_0 - \gamma u)\big) &= y_0 - \gamma u + \gamma\, Tr\big(R \circ G \circ G^{-1}(y_0 - \gamma u)\big) \\ &= y_0 - \gamma u + \gamma\big(Tr\big(R(y_0 - \gamma u)\big)\big) \\ &= y_0 - \gamma u + \gamma\big(u + Tr\big(R(y_0)\big)\big) \\ &= y_0 + \gamma\, Tr\big(R(y_0)\big) = y_0. \end{aligned}$$

The third equality is obtained by applying (12) for $x = y_0$ and taking $-u$ instead of u. The last equality follows from the observation:

$$\begin{aligned} Tr\big(R(y_0)\big) &= Tr\big(R\big(G(x_0) + \gamma\, Tr\big(R\big(G(x_0)\big)\big)\big)\big) \\ &= Tr\big(R\big(G(x_0)\big)\big) - Tr\big(R\big(G(x_0)\big)\big) = 0, \end{aligned}$$

where we use (12) again for $x = G(x_0)$ and $u = Tr(R(G(x_0)))$. Hence we have proved that for any y in the image of F it holds

$$\big\{x \in \mathbb{F}_{p^n} \bigm| F(x) = y\big\} = \big\{G^{-1}(y - \gamma u) \bigm| u \in \mathbb{F}_p\big\},$$

completing the proof. □

Example 3. As a direct consequence of Theorem 3 we get the complete characterization of the linearized permutation polynomials $X + \gamma\, Tr(\beta X) \in \mathbb{F}_{p^n}[X]$. Namely, $X + \gamma\, Tr(\beta X)$ is a permutation polynomial of $\mathbb{F}_{p^n}$ if and only if $Tr(\beta\gamma) \neq -1$. In the remaining cases, when $Tr(\beta\gamma) = -1$, it induces a p-to-1 mapping of $\mathbb{F}_{p^n}$.

Theorem 2 shows that a permutation polynomial of shape (8), where $G(X)$ is a permutation polynomial as well, is obtained by a composition of $G(X)$ with a permutation polynomial given by

$$F(X) = X + \gamma\, Tr\big(R(X)\big), \quad \gamma \in \mathbb{F}_{p^n}. \tag{13}$$

Next we use the results of Section 2 to introduce two classes of permutation polynomials of form (13).

Corollary 1. *Let $\gamma, \beta \in \mathbb{F}_{p^n}$ and $H(X) \in \mathbb{F}_{p^n}[X]$.*

(**i**) *Then the polynomial*

$$F(X) = X + \gamma\, Tr\big(H\big(X^p - \gamma^{p-1}X\big) + \beta X\big)$$

is a permutation polynomial if and only if $Tr(\beta\gamma) \neq -1$.

(**ii**) *Then the polynomial*

$$F(X) = X + \gamma\, Tr\Big(\sum_{u\in\mathbb{F}_p} H(X + u\gamma) + \beta X\Big)$$

is a permutation polynomial if and only if $Tr(\beta\gamma) \neq -1$.

Proof. In both cases, the statement is obvious for $\gamma = 0$. Set $Tr(\beta\gamma) = c$. To prove (**i**), let

$$R(X) = H\big(X^p - \gamma^{p-1}X\big) + \beta X.$$

From Lemma 1 it follows that γ is a c-linear structure of $Tr(R(x))$. More precisely,

$$Tr\big(R(x+\gamma)\big) - Tr\big(R(x)\big) = Tr(\beta\gamma) = c.$$

The rest follows from Theorem 3.

The proof of (**ii**) is obtained similarly by using Lemma 2 instead of Lemma 1. □

Remark 2. Note that if $Tr(\beta\gamma) = -1$ in the statement of Corollary 1 then by Theorem 3 the corresponding mapping $F(x)$ is p-to-1.

Remark 3. The permutation polynomials introduced in Corollary 1 might be of interest for applications. For instance, they are easy to implement if the mapping H is chosen appropriately. Further H may be taken in a way that the resulting mapping F has a desired algebraic degree. For example, permutation polynomials of algebraic degree two are asked in [21] for the design of some public-key cryptosystems.

3.2. Permutations from linearized polynomials

Recall that a polynomial of the form

$$L(X) = \sum_{i=0}^{n-1} \alpha_i X^{p^i}, \quad \alpha_i \in \mathbb{F}_{p^n},$$

is called a *linearized polynomial* over $\mathbb{F}_{p^n}$ and it induces an $\mathbb{F}_p$-linear mapping of $\mathbb{F}_{p^n}$. In this section we characterize the elements $\gamma \in \mathbb{F}_{p^n}$ and polynomials $H(X) \in \mathbb{F}_{p^n}[X]$ for which $L(X) + \gamma\, Tr(H(X))$ is a permutation polynomial. By Proposition 3 the mapping L must necessarily be bijective or p-to-1. Since the case of bijective L is covered in the previous sections, we consider here p-to-1 linear mappings. Recall that a linear mapping is p-to-1 if and only if its kernel is $\alpha\mathbb{F}_p$ for some $\alpha \in \mathbb{F}_{p^n}^*$.

Theorem 4. *Let* $L : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ *be a* p*-to-*1 *linear mapping with kernel* $K = \alpha\mathbb{F}_p$, $\alpha \in \mathbb{F}_{p^n}^*$, *and* $H : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$. *Then the mapping*

$$N(x) = L(x) + \gamma\, Tr\big(H(x)\big), \quad \gamma \in \mathbb{F}_{p^n},$$

is a permutation of $\mathbb{F}_{p^n}$ *if and only if*

- γ *does not belong to the image set of* L, *and*
- $Tr(H(x+\epsilon)-H(x)) \neq 0$ *for any* $x \in \mathbb{F}_{p^n}$ *and* $\epsilon \in K \setminus \{0\}$.

In particular, if $p=2$ *then* $K=\{0,\alpha\}$ *and the second condition means that* α *is a* 1*-linear structure for* $Tr(H(x))$.

Proof. For any $c \in \mathbb{F}_p^*$ we have

$$N(x) = \begin{cases} L(x) & \text{if } Tr(H(x)) = 0, \\ L(x)+\gamma c & \text{if } Tr(H(x)) = c. \end{cases}$$

If γ belongs to the image set of L, say $L(y)=\gamma$, then

$$\gamma c = cL(y) = L(cy) \quad \text{for any } c \in \mathbb{F}_p,$$

so that the image set of N is contained in that of L. In particular, N is not a permutation. We suppose for the rest of the proof that γ does not belong to the image set of L. For all $x \in \mathbb{F}_{p^n}$ and for any $\epsilon \in K \setminus \{0\}$, we have

$$N(x+\epsilon) - N(x) = \gamma\, Tr\big(H(x+\epsilon) - H(x)\big),$$

since $L(\epsilon)=0$. Thus, if N is a permutation, then it must hold

$$Tr\big(H(x+\epsilon) - H(x)\big) \neq 0 \quad \text{for any } x \in \mathbb{F}_{p^n} \text{ and for any } \epsilon \in K \setminus \{0\}, \tag{14}$$

implying the necessity of the second condition.

Conversely, assume that (14) holds. Let $y, z \in \mathbb{F}_{p^n}$ be such that $N(y)=N(z)$. Suppose $Tr(H(y)-H(z))=0$ then

$$N(y) - N(z) = L(y-z) = 0,$$

and thus $y-z \in K$. Further, (14) forces $y=z$. To complete the proof, observe that $Tr(H(y)-H(z))=c$, with $c \neq 0$, would imply

$$N(y) - N(z) = L(y-z) + \gamma c = 0,$$

providing $L(c^{-1}(y-z)) = \gamma$. This contradicts the assumption that γ is not in the image set of L. The case $p=2$ is obviously deduced, completing the proof. □

Remark 4. To apply Theorem 4 we need to check whether γ belongs to the image set of a given p-to-1 mapping $L(x) = \sum_{i=0}^{n-1} \alpha_i x^{p^i}$. We know that the image set of L is a hyperplane $\mathcal{H}_\sigma(0)$. The defining element σ of this hyperplane can be found in terms of the so-called adjoint mapping. Indeed, σ satisfies the following identity:

$$Tr\big(\sigma L(x)\big) = Tr\left(\sigma \sum_{i=0}^{n-1} \alpha_i x^{p^i}\right) = Tr\left(\left(\sum_{i=0}^{n-1} \alpha_i^{p^{n-i}} \sigma^{p^{n-i}}\right) x\right) = 0$$

for any $x \in \mathbb{F}_{p^n}$. Thus σ is the unique nonzero root of the polynomial

$$L^*(X) = \alpha_0 X + \sum_{i=1}^{n-1} \alpha_{n-i}^{p^i} X^{p^i},$$

which is called the *adjoint polynomial* of $L(X)=\sum_{i=0}^{n-1}\alpha_i X^{p^i}$. After having σ, in order to check whether an element γ belongs to the image of L, we need only to verify the condition $Tr(\sigma\gamma)=0$.

Theorem 5. *Let $L:\mathbb{F}_{p^n}\to\mathbb{F}_{p^n}$ be a p-to-1 linear mapping, $K=\alpha\mathbb{F}_p$ be the kernel of L and $\sigma\mathbb{F}_p$ be the kernel of its adjoint mapping L^*. Further let $H:\mathbb{F}_{p^n}\to\mathbb{F}_{p^n}$ and α be a b-linear structure of $Tr(H(x))$. Then*

$$F(x)=L(x)+\gamma\,Tr\big(H(x)\big),\quad \gamma\in\mathbb{F}_{p^n},$$

is a permutation of $\mathbb{F}_{p^n}$ if and only if $Tr(\sigma\gamma)\neq 0$ and $b\neq 0$. Moreover, if $Tr(\sigma\gamma)\neq 0$ and $b=0$ then F is a p-to-1 mapping of $\mathbb{F}_{p^n}$.

Proof. We show that the conditions of Theorem 4 are satisfied if and only if $Tr(\sigma\gamma)\neq 0$ and $b\neq 0$. The condition $Tr(\sigma\gamma)\neq 0$ is equivalent to the requirement that γ does not belong to the image set of L (see Remark 4). Further from Proposition 1 it follows that $c\alpha$ is a cb-linear structure of $Tr(H(x))$, for any $c\in\mathbb{F}_p^*$. Hence, for such a c, we have

$$Tr\big(H(x+c\alpha)-H(x)\big)=cb\neq 0\quad\text{for all } x\in\mathbb{F}_{p^n},$$

which completes the first part of the proof.

Now suppose that $Tr(\sigma\gamma)\neq 0$ and $b=0$. Let x be fixed and y be such that $F(x)=F(y)$. Then we have

$$L(x-y)=\gamma u\quad\text{with } u=Tr\big(H(y)-H(x)\big).$$

If $u\neq 0$ then $L((x-y)/u)=\gamma$ which is impossible. Suppose $u=0$ and thus $x-y\in K=\alpha\mathbb{F}_p$. So $y=x+\alpha v$ for some $v\in\mathbb{F}_p$. Since α is a 0-linear structure of $Tr(H(x))$, it holds $Tr(H(x+c\alpha)-H(x))=0$ for any $c\in\mathbb{F}_p$. This shows that any $y\in x+\alpha\mathbb{F}_p$ satisfies $F(x)=F(y)$. We conclude that $x+\alpha\mathbb{F}_p=\{y\in\mathbb{F}_{p^n}\mid F(x)=F(y)\}$, which implies that F is a p-to-1 mapping of $\mathbb{F}_{p^n}$. □

Next we apply Theorem 5 and Lemmas 1, 2 to describe two classes of permutation polynomials explicitly.

Corollary 2. *Let $\alpha,\beta,\gamma\in\mathbb{F}_{p^n}$, $\alpha\neq 0$ and $H(X)\in\mathbb{F}_{p^n}[X]$.*

(**i**) *Then the polynomial*

$$F(X)=X^p-\alpha^{p-1}X+\gamma\,Tr\big(H\big(X^p-\alpha^{p-1}X\big)+\beta X\big)$$

is a permutation polynomial of $\mathbb{F}_{p^n}$ if and only if $Tr(\gamma\alpha^{-p})\neq 0$ and $Tr(\alpha\beta)\neq 0$.

(**ii**) *Then the polynomial*

$$F(X)=X^p-\alpha^{p-1}X+\gamma\,Tr\Big(\sum_{u\in\mathbb{F}_p}H(X+u\alpha)+\beta X\Big)$$

is a permutation polynomial of $\mathbb{F}_{p^n}$ if and only if $Tr(\gamma\alpha^{-p})\neq 0$ and $Tr(\alpha\beta)\neq 0$.

Proof. The proof follows from Theorem 5 with $L(x)=x^p-\alpha^{p-1}x$. Observe that the kernel of L is $\alpha\mathbb{F}_p$, and the adjoint mapping $L^*(x)=x^{p^{n-1}}-\alpha^{p-1}x$ has the kernel $\alpha^{-p}\mathbb{F}_p$. Further, α is a $Tr(\alpha\beta)$-linear structure of $Tr(H(x^p-\alpha^{p-1}x)+\beta x)$ by Lemma 1, which completes the proof of (**i**). To complete the proof of (**ii**), note that α is a $Tr(\alpha\beta)$-linear structure of $g(x)=Tr(\sum_{u\in\mathbb{F}_p}H(x+u\alpha)+\beta x)$. Indeed,

$$\begin{aligned} g(x+\alpha) &= Tr\Big(\sum_{u\in\mathbb{F}_p} H\big((x+\alpha)+u\alpha\big)+\beta(x+\alpha)\Big)\\ &= Tr\Big(\sum_{u\in\mathbb{F}_p} H\big(x+(u+1)\alpha\big)+\beta x+\beta\alpha\Big)\\ &= \sum_{u\in\mathbb{F}_p} Tr\big(H(x+u\alpha)\big)+Tr(\beta x)+Tr(\beta\alpha)\\ &= g(x)+Tr(\beta\alpha). \qquad \square \end{aligned}$$

Open Problem 2. Find classes of linearized polynomials over $\mathbb{F}_{p^n}$ describing mappings with kernel of dimension 1.

The next theorem shows how changes the dimension of the kernel of a linear mapping after adding to it the mapping $\gamma\, Tr(\beta x)$. In particular, it allows to construct linear mappings with kernel of dimension 1. Recall the notation:

$$\mathcal{H}_\beta(0)=\big\{x\in\mathbb{F}_{p^n}\;\big|\;Tr(\beta x)=0\big\}.$$

Theorem 6. *Let $L_1:\mathbb{F}_{p^n}\to\mathbb{F}_{p^n}$ be a linear mapping with kernel $\mathcal{K}_1$ of dimension k_1, $0\leqslant k_1\leqslant n-1$, over $\mathbb{F}_p$ and $\gamma,\beta\in\mathbb{F}_{p^n}^*$. Define*

$$L(x)=L_1(x)+\gamma\, Tr(\beta x).$$

Then the kernel $\mathcal{K}$ of L has dimension $k\in\{k_1-1,k_1,k_1+1\}$ depending on the cases described below:

(**i**) *γ belongs to the image set of L_1 then*
- *$k=k_1+1$ if $\mathcal{K}_1$ is contained in the hyperplane $\mathcal{H}_\beta(0)$ and there exists an element g satisfying $L_1(g)=\gamma$ and $Tr(\beta g)=-1$;*
- *otherwise $k=k_1$;*

(**ii**) *γ does not belong to the image set of L_1 then*
- *$k=k_1-1$ if $\mathcal{K}_1$ is not contained in the hyperplane $\mathcal{H}_\beta(0)$;*
- *$k=k_1$ if $\mathcal{K}_1$ is contained in the hyperplane $\mathcal{H}_\beta(0)$;*

Proof. The result follows mainly from the fact that any k-dimensional subspace of $\mathbb{F}_{p^n}$ is either contained in $\mathcal{H}_\beta(0)$ or intersects it in a subspace of dimension $k-1$.

(**i**) Observe that the image set of L is contained in that of L_1, and therefore $k\geqslant k_1$. Next we show that if $k>k_1$, then necessarily there exists an element $g\in\mathbb{F}_{p^n}$ such that $L_1(g)=\gamma$ and $Tr(\beta g)=-1$. Indeed, let $x_0\in\mathcal{K}$. Then

$$L_1(x_0)=-\gamma\, Tr(\beta x_0)=-\gamma u,\quad u\in\mathbb{F}_p. \tag{15}$$

If (15) holds only with $u=0$, then $\mathcal{K}\subseteq\mathcal{K}_1$ and $k\leqslant k_1$. Hence there must exist $x_1\in\mathcal{K}$ and $u\in\mathbb{F}_p^*$ such that $Tr(\beta x_1)=u$ and $L_1(x_1)=-\gamma u$. Set $g=-x_1/u$. Then $L_1(g)=\gamma$ and $Tr(\beta g)=-1$. To complete the proof note that with such a g it holds $\mathcal{K}\subseteq\{cg+y\mid c\in\mathbb{F}_p \text{ and } y\in\mathcal{K}_1\}$. For an element $cg+t$, $t\in\mathcal{K}_1$, we have

$$L(cg+t)=L_1(cg)+\gamma\, Tr(\beta cg)+\gamma\, Tr(\beta t)=\gamma\, Tr(\beta t),$$

which shows that $\mathcal{K}=\{cg+y\mid c\in\mathbb{F}_p \text{ and } y\in\mathcal{K}_1\cap\mathcal{H}_\beta(0)\}$.

(**ii**) Suppose that $x_0 \in \mathbb{F}_{p^n}$ belongs to $\mathcal{K}$, i.e. $L(x_0) = L_1(x_0) + \gamma\, Tr(\beta x_0) = 0$. Then, since γ does not belong to the image set of L_1, it must hold $Tr(\beta x_0) = 0$, and consequently $L_1(x_0) = 0$. Thus $x_0 \in \mathcal{K}_1 \cap \mathcal{H}_\beta(0)$. On the other hand, every element of $\mathcal{K}_1 \cap \mathcal{H}_\beta(0)$ belongs to $\mathcal{K}$, completing the proof. □

Next we apply Theorem 6 to describe linearized polynomials inducing p-to-1 mappings on $\mathbb{F}_{p^n}$.

Example 4. Let $n = 2k$ and $\gamma, \beta \in \mathbb{F}_{p^n}^*$. Then the kernel of the linear mapping $L(x) = x^{p^2} - x + \gamma\, Tr(\beta x)$ is of dimension 1 if and only if $Tr_{n/2}(\gamma) \neq 0$ and $Tr_{n/2}(\beta) \neq 0$. Indeed, we apply Theorem 6 for $L_1(x) = x^{p^2} - x$. The kernel $\mathcal{K}_1$ of L_1 is the subfield $\mathbb{F}_{p^2}$ and, in particular, of dimension 2 over $\mathbb{F}_p$. Hence by Theorem 6 the kernel of L is one-dimensional if and only if γ does not belong to the image set of L_1 and $\mathbb{F}_{p^2}$ is not contained in the hyperplane $\mathcal{H}_\beta(0)$. The image set of L_1 consists of elements $y \in \mathbb{F}_{p^n}$ with $Tr_{n/2}(y) = 0$. It remains to note that if $z \in \mathbb{F}_{p^2}$, then

$$Tr(\beta z) = Tr_{2/1}\big(z\, Tr_{n/2}(\beta)\big),$$

and thus $\mathbb{F}_{p^2}$ is contained in $\mathcal{H}_\beta(0)$ if and only if $Tr_{n/2}(\beta) = 0$.

4. Linearized permutation polynomials

In this section we use the results of the previous sections to characterize the linearized permutation polynomials given by $L_1(X) + \gamma\, Tr(L_2(X))$, where both $L_1(X)$ and $L_2(X)$ are linearized polynomials. Firstly, note that the polynomials $Tr(L_2(X))$ and $Tr(L_2^*(1)X)$ describe the same mapping on $\mathbb{F}_{p^n}$, and therefore the problem is reduced to the characterization of permutation polynomials of shape $L_1(X) + \gamma\, Tr(\beta X)$.

Theorem 7. *Let $L_1(X) \in \mathbb{F}_{p^n}[X]$ be a linearized polynomial and $\gamma, \beta \in \mathbb{F}_{p^n}^*$. Then the linearized polynomial*

$$L(X) = L_1(X) + \gamma\, Tr(\beta X)$$

is a permutation polynomial of $\mathbb{F}_{p^n}$ if and only if (**i**) *or* (**ii**) *is fulfilled*:

(**i**) *$L_1(X)$ is a permutation polynomial of $\mathbb{F}_{p^n}$ and $Tr(\beta L_1^{-1}(\gamma)) \neq -1$, where L_1^{-1} is the inverse mapping of L_1;*
(**ii**) *$L_1(X)$ defines a p-to-1 mapping on $\mathbb{F}_{p^n}$ with kernel $\alpha\mathbb{F}_p$. Moreover, γ does not belong to the image set of L_1 and $Tr(\beta\alpha) \neq 0$.*

Proof. It follows from Theorem 6. □

4.1. Linear permutations via semi-bent functions

In this section we apply Theorem 7 to obtain a large set of linearized permutation polynomials over $\mathbb{F}_{2^n}$ from known constructions of semi-bent functions. For the rest of this section, $p = 2$ and n is assumed to be odd. We use the following notation:

$$\mathbf{c} = (c_1, \ldots, c_s), \quad c_i \in \mathbb{F}_{2^n},\ s = \frac{n-1}{2}.$$

The Boolean functions given by

$$f_{\mathbf{c}}(x) = \sum_{i=1}^{\frac{n-1}{2}} Tr\big(c_i x^{2^i+1}\big) \tag{16}$$

are called quadratic Boolean functions on $\mathbb{F}_{2^n}$, since with respect to a fixed basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ such a function has a quadratic multivariate representation. Note that for any $a \in \mathbb{F}_{2^n}$ we have

$$\begin{aligned} f_{\mathbf{c}}(x+a) + f_{\mathbf{c}}(x) &= \sum_{i=1}^{\frac{n-1}{2}} Tr\big(c_i\big(x^{2^i}a + a^{2^i}x + a^{2^i+1}\big)\big) \\ &= Tr\left(\sum_{i=1}^{\frac{n-1}{2}} x\big(c_i a^{2^i} + (c_i a)^{2^{n-i}}\big)\right) + f_{\mathbf{c}}(a) \\ &= Tr\big(xL_{\mathbf{c}}(a)\big) + f_{\mathbf{c}}(a), \end{aligned}$$

where $L_{\mathbf{c}}$ is the linear mapping on $\mathbb{F}_{2^n}$ defined by

$$L_{\mathbf{c}}(x) = \sum_{i=1}^{\frac{n-1}{2}} \big(c_i x^{2^i} + (c_i x)^{2^{n-i}}\big). \tag{17}$$

Definition 2. Let n be odd and $f_{\mathbf{c}}$ and $L_{\mathbf{c}}$ be defined by (16) and (17). Then, $f_{\mathbf{c}}$ is called semi-bent if it has exactly one linear structure or, equivalently, if the linear mapping $L_{\mathbf{c}}(x)$ is 2-to-1 on $\mathbb{F}_{2^n}$.

For more details on semi-bent functions see [3,6,11]. Such functions are studied in terms of sequences in [18, ch. 11]. We want to note also that semi-bent functions are called *three-valued almost optimal* in [3].

The following corollary is an immediate consequence of Theorem 4.

Corollary 3. *Let $f_{\mathbf{c}}$ be semi-bent and α be its (unique) linear structure. Further, let $H : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be such that α is a 1-linear structure of $Tr(H(x))$. Then*

$$N(x) = L_{\mathbf{c}}(x) + \gamma\, Tr\big(H(x)\big) \tag{18}$$

is a permutation of $\mathbb{F}_{2^n}$, for any γ which is not in the image of $L_{\mathbf{c}}$.

From now on, $\mathbf{c}$ is a binary vector and we will use a surprising property of corresponding functions f_c to construct linear permutations or linear mappings which are 2-to-1.

A result by Khoo, Gong and Stinson characterizes all odd integers n for which f_c is semi-bent for *any* nonzero $\mathbf{c} \in \mathbb{F}_2^s$ [11, Section 4].[1] We summarize their results in the next theorem. We denote by $ord_\nu(2)$ the order of 2 modulo ν, that is the smallest k such that ν divides $2^k - 1$.

Theorem 8. *Let ν be an odd prime number and define the properties* (**i**) *and* (**ii**) *as follows*:

(**i**) $ord_\nu(2) = \nu - 1$;
(**ii**) $\nu = 2r + 1$, *r is odd and* $ord_\nu(2) = r$.

Then a function $f_{\mathbf{c}}$ of $\mathbb{F}_{2^n}$ defined by (16) *is semi-bent for any choice of nonzero $\mathbf{c} \in \mathbb{F}_2^s$ if and only if n is an odd prime number satisfying* (**i**) *or* (**ii**).

The first primes satisfying (**i**) or (**ii**) are:

[1] This result was extended to even n in [6].

$$3,\ 5^*,\ 7^*,\ 11^*,\ 13,\ 19,\ 23^*,\ 29,\ 37,\ 47^*,\ 53,\ 59^*,\ 61,\ 67,\ 71,$$

$$79,\ 103,\ 107^*,\ 131,\ 139,\ 149,\ 163,\ 167^*,\ 173,\ 179,\ 181,\ 191$$

where $*$ means that it is a *Sophie Germain prime* (as indicated in [11]).

Remark 5. A prime number ν is said to be a *Sophie Germain prime* if $\nu = 2r + 1$ where r is a prime number too. Suppose that such a prime ν does not satisfy (**i**), so that $ord_\nu(2)$ is a proper divisor of $\nu - 1 = 2r$. Thus $ord_\nu(2) = r$ and (**ii**) holds.

In the next theorem we apply Theorem 8 and Corollary 3 to describe a large family of linear permutations.

Theorem 9. *Let n be an odd prime number satisfying* (**i**) *or* (**ii**). *Let I be a nonempty set of integers in the range* $[1, \frac{n-1}{2}]$. *Then, for any such I the mapping*

$$L_I(x) = \sum_{i\in I}\left(x^{2^i} + x^{2^{n-i}}\right)$$

is 2*-to-*1 *on $\mathbb{F}_{2^n}$ with kernel* $\{0, 1\}$. *Further, for any $\lambda \in \mathbb{F}_{2^n}$, the mapping*

$$N(x) = L_I(x) + Tr(\lambda x)$$

is a linear permutation on $\mathbb{F}_{2^n}$ if and only if $Tr(\lambda) = 1$.

Proof. From Theorem 8 for such an n any $f_{\mathbf{c}}$, with $\mathbf{c} \in \mathbb{F}_2^s$, is semi-bent, and thus any mapping L_I is 2-to-1 (Definition 2). Since $L_I(1) = L_I(0) = 0$, the kernel of L_I is $\mathbb{F}_2$. Further, note that for any I the image of L_I is $\mathcal{H}_1(0)$, since this image is a hyperplane and

$$Tr\big(L_I(x)\big) = \sum_{i\in I} 2 \cdot Tr(x) = 0, \quad \text{for any } x \in \mathbb{F}_{2^n}.$$

Since n is odd, 1 does not belong to $\mathcal{H}_1(0)$. Thus, from Theorem 7, N is a permutation if and only if 1 is a 1-linear structure of $Tr(\lambda x)$ or, equivalently,

$$Tr(\lambda x) + Tr\big(\lambda(x + 1)\big) = Tr(\lambda) = 1. \qquad \square$$

Example 5. Take $n = 7$, which is a Sophie Germain prime. According to Definition 2 and Theorem 8, any linear mapping

$$L_{\mathbf{c}}(x) = \sum_{i=1}^{3}\big(c_i\big(x^{2^i} + x^{2^{7-i}}\big)\big), \quad c_i \in \mathbb{F}_2,$$

is 2-to-1 on $\mathbb{F}_{2^7}$. Its kernel is clearly $\mathbb{F}_2$ and 1 is not in its image. Also, any Boolean function

$$f_{\mathbf{c}}(x) = \sum_{i=1}^{3} Tr\big(c_i x^{2^i+1}\big), \quad c_i \in \mathbb{F}_2,$$

is semi-bent. It has only one nonzero linear structure which is clearly 1 and according to (17)

$$f_{\mathbf{c}}(x+1)+f_{\mathbf{c}}(x)=f_{\mathbf{c}}(1)=Tr\left(\sum_{i=1}^{3}c_i\right)=Tr(w)$$

where w equals the Hamming weight of $\mathbf{c}$ modulo 2. Then, from Corollary 3, any mapping

$$N(x)=\sum_{i=1}^{3}c_i\left(x^{2^i}+x^{2^{7-i}}\right)+Tr\left(\sum_{i=1}^{3}c_i'x^{2^i+1}+(w+1)x\right),\quad c_i,c_i'\in\mathbb{F}_2,$$

is a permutation. On the other hand, it is directly deduced from Theorem 9 that any mapping

$$N(x)=\lambda x+\sum_{i=1}^{3}\left(\left(\lambda^{2^i}+c_i\right)x^{2^i}+\left(\lambda^{2^{7-i}}+c_i\right)x^{2^{7-i}}\right)$$

where $c_i\in\mathbb{F}_2$ and $Tr(\lambda)=1$ is a linear permutation.

5. Conclusion

The main contribution of this paper is the observation that functions with linear structures allow to construct large families of permutation polynomials explicitly. Presently, we are conscious of a number of extensions of our work. Almost all results of this paper can be generalized to polynomials over $\mathbb{F}_q$ of shape $G(X)+\gamma f(X)$, where f induces a mapping from $\mathbb{F}_q$ into an arbitrary its subfield. For more results on such polynomials see [13].

The constructions of permutation polynomials of this paper are based on the existence of linear structures for the involved functions. To determine whether a given function has a linear structure is a difficult problem. In a forthcoming paper we will give a complete solution of this problem for the monomial functions $Tr(\delta x^d)$, extending results from [12].

Acknowledgment

The authors thank the anonymous referees for their detailed comments which improved the clarity of the paper a lot.

References

[1] J. Bierbrauer, G. Kyureghyan, Crooked binomials, Des. Codes Cryptogr. 46 (2008) 269–301.
[2] L. Budaghyan, C. Carlet, G. Leander, Constructing new APN from known ones, Finite Fields Appl. 15 (2) (2009) 150–159.
[3] A. Canteaut, C. Carlet, P. Charpin, C. Fontaine, On cryptographic properties of the cosets of $R(1,m)$, IEEE Trans. Inform. Theory 47 (4) (2001) 1494–1513.
[4] P. Charpin, G. Kyureghyan, On a class of permutation polynomials over $\mathbb{F}_{2^n}$, in: SETA 2008, in: Lecture Notes in Comput. Sci., vol. 5203, Springer-Verlag, Berlin, 2008, pp. 368–376.
[5] P. Charpin, E. Pasalic, On propagation characteristics of resilient functions, in: SAC 2002, in: Lecture Notes in Comput. Sci., vol. 2595, Springer-Verlag, Berlin, 2003, pp. 356–365.
[6] P. Charpin, E. Pasalic, C. Tavernier, On bent and semi-bent quadratic Boolean functions, IEEE Trans. Inform. Theory 51 (12) (2005) 4286–4298.
[7] S. Dubuc, Characterization of linear structures, Des. Codes Cryptogr. 22 (2001) 33–45.
[8] Y. Edel, A. Pott, A new perfect nonlinear function which is not quadratic, Adv. Math. Commun. 3 (1) (2009) 59–81.
[9] J.H. Evertse, Linear structures in block ciphers, in: Advances in Cryptology – EUROCRYPT' 87, in: Lecture Notes in Comput. Sci., vol. 304, Springer-Verlag, Berlin, 1988, pp. 249–266.
[10] H.D.L. Hollmann, Q. Xiang, A class of permutation polynomials of $\mathbb{F}_{2^m}$, Finite Fields Appl. 11 (1) (2005) 111–122.
[11] K. Khoo, G. Gong, D.R. Stinson, A new characterization of semi-bent and bent functions on finite fields, Des. Codes Cryptogr. 38 (2) (2006) 279–295.
[12] G. Kyureghyan, Crooked maps in F_{2^n}, Finite Fields Appl. 13 (3) (2007) 713–726.

[13] G. Kyureghyan, Constructing permutations via linear translators, submitted for publication, available on arXiv:0903.0743.
[14] G. Kyureghyan, Y. Tan, A family of planar mappings, in: Enhancing Crypto-Primitives with Techniques from Coding Theory, IOS Press, 2009, pp. 175–179.
[15] X. Lai, Additive and linear structures of cryptographic functions, in: FSE 94, in: Lecture Notes in Comput. Sci., vol. 1008, Springer-Verlag, Berlin, 1995, pp. 75–85.
[16] Y. Laigle-Chapuy, Permutation polynomials and applications to coding theory, Finite Fields Appl. 13 (1) (2007) 58–70.
[17] R. Lidl, H. Niederreiter, Finite Fields, Encyclopedia Math. Appl., vol. 20, Addison–Wesley, Reading, MA, 1983.
[18] R.J. McEliece, Finite Fields for Computer Scientists and Engineers, Kluwer, Boston, 1987.
[19] W. Meier, O. Staffelbach, Nonlinearity criteria for cryptographic functions, in: Advances in Cryptology – EUROCRYPT' 89, in: Lecture Notes in Comput. Sci., vol. 434, Springer-Verlag, Berlin, 1990, pp. 549–562.
[20] H. Niederreiter, K.H. Robinson, Complete mappings of finite fields, J. Aust. Math. Soc. Ser. A 33 (1982) 197–212.
[21] J. Patarin, Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms, in: Advances in Cryptology – EUROCRYPT' 96, in: Lecture Notes in Comput. Sci., vol. 1070, Springer-Verlag, Berlin, 1996, pp. 549–562.
[22] V.V. Yashchenko, On the propagation criterion for Boolean functions and bent functions, Probl. Inf. Transm. 33 (1) (1997) 62–71.
[23] J. Yuan, C. Ding, H. Wang, J. Pieprzyk, Permutation polynomials of the form $(x^p - x - \delta)^s + L(x)$, Finite Fields Appl. 14 (4) (2008) 482–493.